ABSTRACT

A method for authenticating and negotiating security parameters among two or more network devices is disclosed. The method has a plurality of modes including a plurality of messages exchanged between the two or more network devices. In a main mode, the two or more network devices establish a secure channel and select security parameters to be used during a quick mode and a user mode. In the quick mode, the two or more computers derive a set of keys to secure data sent according to a security protocol. The optional user mode provides a means of authenticating one or more users associated with the two or more network devices. A portion of the quick mode is conducted during the main mode thereby minimizing the plurality of messages that need to be exchanged between the initiator and the responder.